

DEPARTMENT OF WORKFORCE DEVELOPMENT
DIVISION OF WORKFORCE SOLUTIONS
ADMINISTRATOR'S MEMO SERIES

ACTION 01-24

ISSUE DATE: 12/18/2001
DISPOSAL DATE: 12/31/2001

RE: PROCESS FOR GRANTING
DWS AUTOMATED
SYSTEMS ACCESS

To: Income Maintenance Agency Directors
W-2 Agency Directors
Child Support Agency Directors
Job Service District Directors
Workforce Development Board Directors

From: Eric Baker /s/
Administrator

DWS Administrators Memo-Procedures for Access to Division of Workforce Solutions (DWS)
Automated Systems

This memo provides each Job Service District (JSD) and Workforce Development Board (WDB) with updated procedures for requesting access to the former DWE automated information systems. Currently, DWS has a process model for requesting access to the Client Assistance for Re-employment and Economic Support (CARES), and the Kids Information Data System (KIDS). It has been endorsed by the Department of Workforce Development (DWD) legal counsel and will be expanded to cover access to the Government Services Tracking And Reporting System (G*STARS), the Employer Records System (ERS), and the Wisconsin Job Order System (WJOS). These are the automated systems covered in this memo. Because they already operate under the DWS model, this memo is being sent to Income Maintenance, W-2, and Child Support Agency directors for informational purposes only.

With the merger of the former Division of Economic Support and Division of Workforce Excellence, came the consolidation of security responsibilities for the new division. Responsibility for security in the Division of Workforce Solutions has been assigned to the Automated Operations Section (AOS) within the Bureau of Workforce Programs (BWP). AOS is responsible for administration of the access model described below.

DWS Data Steward

The DWD has a standing policy regarding access to confidential client information contained in various automated systems. As a matter of public trust, it is our responsibility to ensure that reasonable steps are taken to safeguard sensitive client and administrative information. It is policy that each DWD division administrator appoint a data steward for each of its major automated data systems. Within DWS, there are two appointed data stewards. One is responsible for CARES, G*STARS, ERS, and WJOS. The other is responsible for KIDS. They are both located in the DWS central office. The role of a data steward is to insure that access to

confidential client information is only permitted under legal circumstance and only for a legitimate business need. To accomplish this, a data steward engages in the following:

- negotiates data exchange agreements with entities that have any type of access to data, whether it is on-line, one-time requests, or recurring exchange of extract files;
- oversees requests for on-line access and requests for access to specific data;
- determines appropriate level of access based on business need;
- ensures access to data is legal and will consult with the department's legal counsel in questionable cases;
- works closely with the division's security officer and policy staff when investigating questionable requests for access;
- provides input to the DWD data administrator on each data exchange agreement that DES enters, providing the description, purpose, legal authority, justification, anticipated results, and estimated cost savings (if there are any) to the Public Records Board. DWD is required to report this information to the Public Records Board as required by section 19.69 of Wisconsin Statutes.

Data Exchange Agreements

Data exchange agreements are confidentiality agreements between DWS and its internal and external partner agencies. Data exchange agreements enumerate the business purpose for access to confidential client information. The agreements form a chain of accountability, which hold agencies (and their partner agencies) to strict confidentiality requirements. If security requirements are violated, and confidential client information is compromised, the agreement spells out corrective action steps that will be taken up to, and including, the termination of system access and referral to legal authority for possible criminal prosecution.

Individual data exchange agreements are non-financial agreements signed by the DWS administrator (and in some instances the department secretary) and another entity's designated administrative official. The United States Department of Agriculture (USDA), for example, requires the department secretary to sign their agreement. Agreements must be in place before access to data can commence. Agreements spell out the level of access (i.e., query or change) and may specify specific screens within a given system to which access is granted.

DWS Security Officer

The DWS Security Officer is responsible for processing all computer access request forms to the systems previously listed in this memo. Upon receipt of an access request form, the security officer will verify the request is valid and then assign a logon ID and password. Whenever a questionable request is received, it is the DWS security officer's responsibility to follow up with the requesting agency's security officer to ensure only individuals with a legitimate business need are granted the appropriate access.

Action Items

Each Job Service District and Workforce Development Board must appoint a security officer who will be responsible, within their respective organizations, for approving all computer access requests. It is suggested a back-up security officer also be appointed to approve requests when the security officer is unavailable. A DES-11652 should be filled out and submitted to the DWS Security Officer. A copy is attached to this memo and can also be found at the following URL: http://dwdworkweb/des/partner_forms.htm

Since there are multiple offices within a JSD and WDB, it is suggested each office appoint a Functional Area Security Liaison (FASL). This person would be responsible for review and approval of all access requests from their individual office. The form would be forwarded to the JSD or WDB security officer for approval. The JSD or WDB security officer will then mail or fax the form to the DWS Security Officer for processing.

Each WDB will appoint an agreement coordinator to work with the DWS Data Steward to consummate a data sharing agreement with the department, including the creation and maintenance of a list of partners. A draft of such an agreement is attached to this memo. The name and contact information of the DWS Data Steward is listed in Attachment A of the attached draft agreement. It is suggested that each WDB have an agreement with each of its partners. A WDB partner is defined as an entity providing services under contract to the board. A draft of a WDB-Partner Agreement is also attached to this memo.

WDB Security Officers are authorized to approve access requests for G*STARS, ERS, and limited query access to CARES. There must be a legitimate business need for granting query access to CARES, documented in a data sharing agreement, and approved by the DWS Data Steward, before approval authority will be given to the WDB Security Officer. Requests for CARES query access from a WDB partner must be approved by the WDB Security Officer before being submitted to the DWS Security Officer for processing. Ultimately, each WDB is responsible for ensuring their partners safeguard confidential client information. The agreement between the WDB and its partner(s) will document what is expected of a partner agency as it relates to safeguarding confidential client information.

Each JSD must submit a list of partner agencies and a contact person for each agency to the DWD data steward listed in Attachment A of the attached draft agreement. The DWD Data Steward will consummate a data sharing agreement with each partner. A JSD partner is defined as a participant in the delivery of One Stop Operator (OSO) services recognized within the district. In most instances, these will be agencies the JSD is subcontracting with for services. But in the case of access to WJOS, the definition of partner may or may not involve a subcontract.

Because of their WIA Title III responsibilities, only JSD's security officer may approve access requests for WJOS. In addition, they are authorized to approve access requests for G*STARS, ERS, and limited query access to CARES. There must be a legitimate business need for granting query access to CARES, documented in a data sharing agreement, and approved by the DWS Data Steward, before approval authority will be given to the JSD Security Officer. Requests for CARES query access from a JSD partner must be approved by the JSD Security Officer before being submitted to the DWS Security Officer for processing. Ultimately, each JSD is responsible for ensuring their partners safeguard confidential client information. A data sharing agreement between the DWD and your partner(s) will document what is expected of a partner agency as it relates to safeguarding confidential client information.

Under no circumstances will a WDB or JSD Security Officer be granted authority to approve update access to CARES. Authorization for approving update access is restricted to an Income Maintenance Agency or W-2 Agency Security Officer.

Computer Access Request Form

Starting February 1, 2002, Job Service Districts and Workforce Development Boards will be required to submit a DES 10 Computer Access Request for new staff and staff

that are terminating or job duties have changed and whose access needs to DWS automated systems change. A DES 11 Computer Access Request Supplement will be used to change the level of an individual's access to CARES. These forms can be found on the DWS partner page using the following URL:

http://dwdworkweb/des/partner_forms.htm. Both forms have been revised to include the former DWE systems.

More detailed information on the DWS Security Policies and Procedures and the role of a security officers and FASL can be found in the DES Security Manual. The manual is being revised to incorporate the former DWE systems that are now part of the DWS.

The manual can be found on the DWS partner page using the following URL:

<http://dwdworkweb/des/manuals/des/securman.htm>.

REGIONAL OFFICE CONTACT: Area Administrators

Attachment(s)